915-008.012
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: A. Kiiveri et al
Serial No.: 0 / 10/634,734 Group No.:
Filed: August 4, 2003 Examiner:
For: Secure Execution Architecture

Commissioner of Patents and Trademarks
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country :International Bureau
Application Number :PCT/IB02/03216
Filing Date :August 13, 2002

Reg. No. 31,391

Francis Maguire
SIGNATURE OF ATTORNEY
Francis J. Maguire
Type or print name of attorney

Tel. No. (203) 261-1234

WARE, FRESSOLA, VAN DER SLUYS & ADOLPHSON
P.O. Address
755 Main Street, PO Box 224
Monroe CT 06468

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

CERTIFICATE OF MAILING (37 CFR 1.8a).

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the: Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Date: Sept. 29, 2003

Margery B. Hood
(Type or print name of person mailing paper)

Margery B. Hood
(Signature of person mailing paper)

WORLD INTELLECTUAL PROPERTY ORGANIZATION
ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
34, chemin des Colombettes, Case postale 18, CH-1211 Genève 20 (Suisse)
Téléphone: (41 22) 338 91 11 - e-mail: wipo.mail @ wipo.int. - Fac-similé: (41 22) 733 54 28

PATENT COOPERATION TREATY (PCT)
TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

CERTIFIED COPY OF THE INTERNATIONAL APPLICATION AS FILED AND OF ANY CORRECTIONS THERETO

COPIE CERTIFIÉE CONFORME DE LA DEMANDE INTERNATIONALE, TELLE QU'ELLE A ÉTÉ DÉPOSÉE, AINSI QUE DE TOUTES CORRECTIONS Y RELATIVES

International Application No. Demande internationale n°	PCT/IB02/03216	International Filing Date Date du dépôt international	13 August 2002 (13.08.02)

Geneva/Genève,

02 September 2003
(02.09.03)

International Bureau of the
World Intellectual Property Organization (WIPO)

Bureau International de l'Organisation Mondiale
de la Propriété Intellectuelle (OMPI)

J.-L. Baron
Head, PCT Receiving Office Section
Chef de la section "office récepteur du PCT"

PCT
REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

For receiving Office use only
PCT / IB 02 / 03216
International Application No.

13 AUG 2002 (13.08.02)
International Filing Date

INTERNATIONAL BUREAU OF WIPO
PCT International Application
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference (if desired)(12 characters maximum) PC-2018600

Box No. I TITLE OF INVENTION

SECURE EXECUTION ARCHITECTURE

Box No. II APPLICANT ☐ This person is also inventor.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

NOKIA CORPORATION
Keilalahdentie 4
FI-02150 ESPOO
Finland

Telephone No.

Facsimile No.

Teleprinter No.

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Finland

State *(that is, country)* of residence: Finland

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

PAATERO, Lauri
Rikalantie 4
FIN-00970 Helsinki
Finland

This person is:
☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Finland

State *(that is, country)* of residence: Finland

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

AWAPATENT AB
Box 45086
SE-104 30 STOCKHOLM
SWEDEN

Telephone No.
+46 8 440 95 00

Facsimile No.
+46 8 440 95 50

Teleprinter No.

Agent's registration No. with the Office

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent

Sheet No. 2

Continuation of Box No. III **FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)**

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

KIIVERI, Antti
Peikontie 1 F 72
FIN-90550 Oulu
Finland

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Finland
State *(that is, country)* of residence: Finland

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:
State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:
State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:
State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on another continuation sheet.

Sheet No. 3

Box No. V DESIGNATION OF STATES *Mark the applicable check-boxes below; at least one must be marked.*

The following designations are hereby made under Rule 4.9(a):

Regional Patent

☒ **AP** **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZM Zambia, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT *(if other kind of protection or treatment desired, specify on dotted line)*

☒ **EA** **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

☒ **EP** **European Patent:** AT Austria, BE Belgium, BG Bulgaria, CH and LI Switzerland and Liechtenstein, CY Cyprus, CZ Czech Republic, DE Germany, DK Denmark, EE Estonia, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, SK Slovakia, TR Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☒ **OA** **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GQ Equatorial Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)*

National Patent *(if other kind of protection or treatment desired, specify on dotted line):*

☒	AE	United Arab Emirates	☒	GM	Gambia	☒	NZ	New Zealand	
☒	AG	Antigua and Barbuda	☒	HR	Croatia	☒	OM	Oman	
☒	AL	Albania	☒	HU	Hungary	☒	PH	Philippines	
☒	AM	Armenia	☒	ID	Indonesia	☒	PL	Poland	
☒	AT	Austria +Utility Model	☒	IL	Israel	☒	PT	Portugal	
☒	AU	Australia	☒	IN	India	☒	RO	Romania	
☒	AZ	Azerbaijan	☒	IS	Iceland	☒	RU	Russian Federation	
☒	BA	Bosnia and Herzegovina	☒	JP	Japan				
☒	BB	Barbados	☒	KE	Kenya	☒	SD	Sudan	
☒	BG	Bulgaria	☒	KG	Kyrgyzstan	☒	SE	Sweden	
☒	BR	Brazil	☒	KP	Democratic People's Republic of Korea	☒	SG	Singapore	
☒	BY	Belarus				☒	SI	Slovenia	
☒	BZ	Belize	☒	KR	Republic of Korea	☒	SK	Slovakia +Utility Model	
☒	CA	Canada	☒	KZ	Kazakhstan	☒	SL	Sierra Leone	
☒	CH & LI	Switzerland and Liechtenstein	☒	LC	Saint Lucia	☒	TJ	Tajikistan	
☒	CN	China	☒	LK	Sri Lanka	☒	TM	Turkmenistan	
☒	CO	Colombia	☒	LR	Liberia	☒	TN	Tunisia	
☒	CR	Costa Rica	☒	LS	Lesotho	☒	TR	Turkey	
☒	CU	Cuba	☒	LT	Lithuania	☒	TT	Trinidad and Tobago	
☒	CZ	Czech Republic +Utility Model	☒	LU	Luxembourg				
☒	DE	Germany +Utility Model	☒	LV	Latvia	☒	TZ	United Republic of Tanzania	
☒	DK	Denmark +Utility Model	☒	MA	Morocco	☒	UA	Ukraine	
☒	DM	Dominica	☒	MD	Republic of Moldova	☒	UG	Uganda	
☒	DZ	Algeria				☒	US	United States of America	
☒	EC	Ecuador	☒	MG	Madagascar				
☒	EE	Estonia +Utility Model	☒	MK	The former Yugoslav Republic of Macedonia	☒	UZ	Uzbekistan	
☒	ES	Spain				☒	VN	Viet Nam	
☒	FI	Finland +Utility Model	☒	MN	Mongolia	☒	YU	Yugoslavia	
☒	GB	United Kingdom	☒	MW	Malawi	☒	ZA	South Africa	
☒	GD	Grenada	☒	MX	Mexico	☒	ZM	Zambia	
☒	GE	Georgia	☒	MZ	Mozambique	☒	ZW	Zimbabwe	
☒	GH	Ghana	☒	NO	Norway				

Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:

☐	☐	☐
☐	☐	☐

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM

The priority of the following earlier application(s) is hereby claimed:

	Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country or member of WTO	regional application:* regional Office	international application: receiving Office
item (1)					
item (2)					
item (3)					
item (4)					
item (5)					

☐ Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as:

☐ all items ☐ item (1) ☐ item (2) ☐ item (3) ☐ item (4) ☐ item (5) ☐ other, see Supplemental Box

* *Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):* ....

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)*:

ISA / EPO

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*:

Date *(day/month/year)* Number Country *(or regional Office)*

Box No. VIII DECLARATIONS

The following **declarations** are contained in Boxes Nos. VIII (i) to (v) *(mark the applicable check-boxes below and indicate in the right column the number of each type of declaration)*: Number of declarations

☐ Box No. VIII (i)	Declaration as to the identity of the inventor	:
☐ Box No. VIII (ii)	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	:
☐ Box No. VIII (iii)	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	:
☐ Box No. VIII (iv)	Declaration of inventorship (only for the purposes of the designation of the United States of America)	:
☐ Box No. VIII (v)	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	:

Sheet No. 5

Box No. IX CHECK LIST; LANGUAGE OF FILING

This international application contains:

(a) the following number of **sheets in paper form:**

request (including declaration sheets)	: 5
description (excluding sequence listing part)	: 12
claims	: 3
abstract	: 1
drawings	: 2
Sub-total number of sheets	: 23
sequence listing part of description *(actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (b) below)*	:
Total number of sheets	:

(b) sequence listing part of description filed in **computer readable form**

(i) ☐ only (under Section 801(a)(i))

(ii) ☐ in addition to being filed in paper form (under Section 801(a)(ii))

Type and number of carriers (diskette, CD-ROM, CD-R or other) on which the sequence listing part is contained *(additional copies to be indicated under item 9(ii), in right column)*:

.....

This international application is **accompanied** by the following item(s) *(mark the applicable check-boxes below and indicate in right column the number of each item)*: — Number of items

1. ☐ fee calculation sheet :
2. ☐ original separate power of attorney :
3. ☐ original general power of attorney :
4. ☒ copy of general power of attorney; reference number, if any: GPA 02/0021 :
5. ☐ statement explaining lack of signature :
6. ☐ priority document(s) identified in Box No. VI as item(s): :
7. ☐ translation of international application into *(language)*: :
8. ☐ separate indications concerning deposited microorganism or other biological material :
9. ☐ sequence listing in computer readable form (indicate also type and number of carriers (diskette, CD-ROM, CD-R or other))
   (i) ☐ copy submitted for the purposes of international search under Rule 13*ter* only (and not as part of the international application) :
   (ii) ☐ *(only where check-box (b)(i) or (b)(ii) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Rule 13*ter* :
   (iii) ☐ together with relevant statement as to the identity of the copy or copies with the sequence listing part mentioned in left column :
10. ☐ other *(specify)*: .....

Figure of the drawings which should accompany the abstract: 1

Language of filing of the international application: English

Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Stockholm 13 August 2002

Lars Ellner

Lars Ellner

Authorized Representative

For receiving Office use only

1. Date of actual receipt of the purported international application:	13 AUG 2002 (13.08.02)	2. Drawings: ☐ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		
4. Date of timely receipt of the required corrections under PCT Article 11(2):		
5. International Searching Authority (if two or more are competent): ISA/ EP	6. ☒ Transmittal of search copy delayed until search fee is paid.	

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

SECURE EXECUTION ARCHITECTURE

Technical Field of the Invention

The present invention relates to circuitry for providing data security, which circuitry contains at least one processor and at least one storage circuit. The present invention also relates to a method for providing data security in circuitry containing at least one processor and at least one storage circuit.

Background Art

Various electronic devices, such as mobile telecommunication terminals, portable computers and PDAs require access to security related components such as application programs, cryptographical keys, cryptographical key data material, intermediate cryptographical calculation results, passwords, authentication of externally downloaded data etc. It is often necessary that these components, and the processing of them, is kept secret within the electronic device. Ideally, they shall be known by as few people as possible. This is due to the fact that a device, for example a mobile terminal, could possibly be tampered with if these components are known. Access to these types of components might aid an attacker with the malicious intent to manipulate a terminal.

Further, in the devices, these above mentioned security related components will be handled, processed and managed alongside more general components which do not require any secure processing. Therefore, a secure execution environment is introduced in which environment a processor within the electronic device is able to access the security related components. Access to the secure execution environment, processing in it and exit from it should be carefully controlled. Prior art hardware comprising this secure environment is often enclosed within a tamper resistant packaging. It should

not be possible to probe or perform measurements and tests on this type of hardware which could result in the revealing of security related components and the processing of them.

An electronic device processing information in a secure environment and storing security related information in a secure manner is shown in US patent No. 5,892,900. The patent discloses a virtual distribution environment securing, administering and controlling electronic information use. It comprises a rights protection solution for distributors, financial service providers, end-users and others. The invention uses electronic devices called Secure Processing Units to provide security and secure information storage and communication. Such a device, including a processor, is enclosed within a "tamper resistant security barrier", separating the secure environment from the outer world. The electronic device provides both the secure environment and an unsecure environment, in which latter case the processor of the device has no access to the security related information.

A problem that has to be solved is to enable for a third party to perform testing, debugging and servicing of the electronic device and its software without risking that the third party is given access to information which makes it possible to manipulate the security related components of the device so as to affect the security functions when in the secure environment. It should be possible to move between the two environments smoothly, without having to initialize one or the other every time a movement is effected.

Summary of the Invention

It is an object of the present invention to provide a solution to the above given problem by proposing an architecture comprising a secure environment in which it is possible to store and process information such as cryptographical keys and other security related data in a secure way and still making it possible to test and debug the architecture and its accompanying software in an unsecure environment without giving access to the security data.

This object is attained by the invention in a first aspect in the form of circuitry for providing data security, which circuitry contains at least one processor and at least one storage circuit according to claim 1 and in a second aspect in the form of a method for providing data security in circuitry containing at least one processor and at least one storage circuit according to claim 7. Preferred embodiments are defined by the dependent claims.

According to the first aspect of the invention, circuitry is provided comprising at least one storage area in a storage circuit, in which storage area protected data relating to circuitry security are located. The circuitry is arranged with mode setting means arranged to place a processor comprised in the circuitry in one of at least two different operating modes, the mode setting means being capable of altering the processor operating modes. Further, it comprises storage circuit access control means arranged to control the processor to gain access to the storage area in which protected data are located based on a first processor operating mode, and arranged to prevent the processor from accessing the storage area in which protected data are located, based on a second processor operating mode, thereby enabling the processor to execute non-verified software downloaded into the circuitry.

According to the second aspect of the invention, a method is provided wherein protected data relating to circuitry security is stored in a storage circuit. A processor is set in one of at least two different alterable operating modes. The method further comprises the step of enabling the processor to access a storage area in which the protected data are located by setting the processor in a first operating mode and preventing the processor from accessing the storage area in which protected data are located by setting the processor in a second operating mode, thereby enabling the processor to execute non-verified software downloaded into the circuitry.

The invention is based on the idea that circuitry is provided in which a processor is operable in at least two different modes, one first secure operating mode and one second unsecure operating mode. In the secure mode, the processor has access to security related data located in various memories located within the circuitry. The security data include cryptographical keys and algorithms, software for booting the circuitry, secret data such as random numbers used as cryptographical key material, application programs etc. The circuitry can advantageously be used in mobile telecommunication terminals, but also in other electronic devices such as computers, PDAs or other devices with need for data protection. In the case where the circuitry is placed within a mobile telecommunication terminal, it might be desirable that the circuitry provides the terminal with a unique identification number and accompanying keys for cryptographic operations on the identification number. The access to these security data and the processing of them need to be restricted, since an intruder with access to security data could manipulate the terminal. When testing and/or debugging the terminal, access to security information is not allowed. For this reason, the processor is placed in the unsecure operating mode, in

which mode it is no longer given access to the protected data.

The invention advantageously enables the processor of the circuitry to execute non-verified software downloaded into the circuitry. This allows testing, debugging and servicing of the electronic device and its software without risking that a third party is given access to information which makes it possible to manipulate the security related components of the device so as to affect the security functions when in the secure environment.

It should be noted that in US patent No. 5,892,900, the unsecure mode is the "normal" mode, used when transactions and communications must be secure, whereas in the present invention, the secure mode is the normal mode. In the present invention, unsecure mode is only entered during testing and/or debugging or other types of special cases when security data must be protected, i.e. when secure mode can not be practically maintained.

The present invention eliminates the use for special purpose terminals adapted for use in research and development. During a development stage, it is sometimes a requirement to be able to download untrusted and/or unchecked code into terminals. By enabling the unsecure mode, a channel is provided into the terminal without giving access to security related components. Consequently, the same terminal can be utilized for normal operation as well as in the development stage. It should be understood that it is rather expensive to manufacture special purpose terminals.

According to an embodiment of the invention, the circuitry of the invention is arranged with a timer controlling the time period during which the processor is in the unsecure mode. If other security controlling actions should fail, a maximum given time period is set during which access is given to unsecure processor mode. This restrains the possibility for an intruder to perform debugging and testing of the device.

According to another embodiment of the invention, authentication means are provided, which means being arranged to authenticate data externally provided to the terminal. An advantage with this feature is that during the manufacturing stage, and other stages where normal, secure operating mode is not yet activated, the terminal can be used for a limited time period, sufficient to load accepted, signed code into the terminal. It is also possible to download signed code packages into the terminal during secure mode operation. This facilitates the possibility to add new security features to the terminal, bringing flexibility to the architecture. The architecture enables the applications to be divided into secure and unsecure parts. The circuit checks the code packages which are signed appropriately. Secure applications are downloaded to, and executed from, the storage area holding the protected data. This makes downloading of data smoother. If this feature was not present, it would be necessary to download secure applications and unsecure applications separately.

According to yet another embodiment of the invention, the circuitry is arranged with means for indication of the mode in which the processor is operating. It is appropriate that a mode register is set within the circuitry, keeping track of the current mode. In case the circuitry is arranged within a mobile telecommunication terminal, it should be possible to indicate on the terminal display, via the terminal loudspeaker or in any other visual way, to a terminal user the fact that the terminal is operating in unsecure mode. This will draw the user's attention to the fact that unsecure mode has been entered.

In accordance to further embodiments of the present invention, the mode setting means arranged to control the modes of the processor comprise an application program. This has the advantage that the mode could be set by the device itself, not having to rely on external signals.

From a security viewpoint, this is preferable since by controlling the application software, the setting of processor modes can also be controlled. It is also possible to have an external signal connected to the circuitry, by which signal it is possible to control the processor mode. By using an external signal, a mode change can be executed easy and fast, which can be advantageous in test environments. A combination of these two mode setting means is feasible.

Brief Description of the Drawings

The present invention will be described in greater detail with reference to the following drawings, wherein:

Fig. 1 shows a block scheme of a preferred embodiment of circuitry for providing data security according to the present invention; and

Fig. 2 shows a flow chart of a boot process for the circuitry according to the present invention.

Description of Preferred Embodiments of the Invention

Fig. 1 shows a block scheme of a preferred embodiment of the present invention. As can be seen, the architecture in Fig. 1 contains both software and hardware. The architecture is implemented in the form of an ASIC (Application Specific Integrated Circuit). The processing part of the architecture contains a CPU and a digital signal processor DSP. These two processor can be merged into one single processor. Normally the CPU handles communication operations and the DSP handles the computation of data.

The secure environment comprises a ROM from which the ASIC is booted. This ROM contains boot application software and an operating system OS. The operating system controls and executes applications and offers various security services to the applications such as control of application software integrity and access control. The operating system has access to the ASIC hardware and it

cannot itself provide rigorous hardware security, but it must rely on the security architecture.

Certain application programs residing in the secure environment, i.e. the protected data storage area, has precedence over other application programs. In a mobile telecommunication terminal, in which the ASIC can be arranged, a boot software should exist, which software includes the main functionality of the terminal. It is not possible to boot the terminal to normal operating mode without this software. This has the advantage that by controlling this boot software, it is also possible to control the initial activation of every terminal.

The secure environment also comprises RAM for storage of data and applications. The RAM preferably stores so called protected applications, which are smaller size applications for performing security critical operations inside the secure environment. Normally, the way to employ protected applications is to let "normal" applications request services from a certain protected application. New protected applications can be downloaded into the secure environment at any time, which would not be the case if they would reside in ROM. Secure environment software controls the download and execution of protected applications. Only signed protected applications are allowed to run. The protected applications can access any resources in the secure environment and they can also communicate with normal applications for the provision of security services.

In the secure environment, a fuse memory is comprised containing a unique random number that is generated and programmed into the ASIC during manufacturing. This random number is used as the identity of a specific ASIC and is further employed to derive keys for cryptographic operations. Further, storage circuit access control means in the form of a security control register is arranged. The purpose of the security control register is to give the CPU access to the secure environment, or

preventing the CPU from accessing the secure environment, depending on the mode set in the register. The processor operating modes can be set in the register by application software, resulting in the fact that the architecture does not have to rely on external signals. From a security viewpoint, this is preferable since by controlling the application software, the setting of processor modes can also be controlled. It is also possible to have an external signal (not shown) connected to the ASIC, by which signal it is possible to set the security control register. By using an external signal, a mode change can be executed easy and fast, which can be advantageous in test environments. A combination of these two mode setting means is feasible.

Preferably, the mobile telecommunication terminal should indicate on the terminal display, via the terminal loudspeaker or in any other visual way, to a terminal user the fact that the terminal is operating in unsecure mode. This will make the user aware of the fact that unsecure mode has been entered.

A watchdog is arranged for various timer purposes. In case signature verification of downloaded software fails, checksums does not match or some other error is detected, the operation of the ASIC, or the mobile telecommunication terminal it is arranged in, should stop. This should preferably not be done immediately when the error occurs. A random timeout, e.g. different time spans up to 30 seconds, is desired. This makes it more difficult for an attacker to detect the instant at which the terminal has detected the error. The disabling of watchdog updating is set in the security control register. The result of this operation is that the terminal will reset itself. The watchdog can also control the time period during which the processor is in the unsecure mode. If other security controlling actions should fail, a maximum given time period is set during which access is given to unsecure processor mode. This restrains the possibility

for an intruder to perform debugging and testing of the device.

The CPU is connected to the secure environment hardware via a memory management unit MMU that handles memory operations. It also maps virtual addresses to physical addresses in memory for processes executed in the CPU. The MMU is located on a bus containing data, address and control signals. It is also possible to have a second MMU arranged to handle the memory operations for the ASIC RAM located outside the secure environment. A standard bridge circuit for limitation of data visibility on the bus is arranged within the ASIC. The architecture should be enclosed within a tamper resistant packaging. It should not be possible to probe or perform measurements and tests on this type of hardware which could result in the revealing of security related components and the processing of them. The DSP has access to other peripherals such as a direct memory access (DMA) unit. DMA is provided by the architecture to allow data to be sent directly from the DSP to a memory. The DSP is freed from involvement with the data transfer, thus speeding up overall operation. Other peripherals such as RAMs, flash memories and additional processors can be provided outside the ASIC. A RAM is also arranged outside the secure environment in the ASIC, which RAM holds the non-verified software executed by the CPU.

By providing the above described architecture in which the CPU is operable in two different modes, one secure operating mode and one unsecure operating mode, the CPU of the architecture can be enabled to execute non-verified software downloaded into the ASIC. This is due to the fact that only verified software has access to the secure environment. This allows testing, debugging and servicing of the mobile telecommunication terminal and its software without risking that a third party is given access to information which makes it possible to manipulate the security related components of the device

so as to affect the security functions when in the secure environment.

In the secure mode, the processor has access to security related data located within the secure environment. The security data include cryptographical keys and algorithms, software for booting the circuitry, secret data such as random numbers used as cryptographical key material, application programs etc. The circuitry can advantageously be used in mobile telecommunication terminals, but also in other electronic devices such as computers, PDAs or other devices with need for data protection. The access to these security data and the processing of them need to be restricted, since an intruder with access to security data could manipulate the terminal. When testing and/or debugging the terminal, access to security information is not allowed. For this reason, the processor is placed in the unsecure operating mode, in which mode it is no longer given access to the protected data within the secure environment.

Fig. 2 illustrates a flow chart of the power up boot process for the architecture. At power up, ROM boot software activates secure mode for initial configuration. Then, signatures for the first protected application and operating system to be downloaded are checked. If the signatures are correct, the application and the operating system is downloaded into the secure environment RAM. When the desired software has been downloaded, the CPU is informed that the download is completed and the CPU starts executing the verified software. The operating system and protected application have thus been downloaded into the secure environment in a secure and trusted manner.

However, if the signature check fails or if no signature is present, unsecure mode is activated and the non-verified application is loaded into the ASIC RAM located outside the secure environment. Possibly, the watchdog is set to limit the time period during which the

unsecure mode is activate. A maximum time period is set during which the unsecure mode is active. When boot is completed, this non-verified application is executed by the CPU. The secure environment is now inaccessible.

Even though the invention has been described with reference to specific exemplifying embodiments thereof, many different alterations, modifications and the like will become apparent for those skilled in the art. The described embodiments are therefore not intended to limit the scope of the invention, as defined by the appended claims.

CLAIMS

1. Circuitry for providing data security, which circuitry contains at least one processor and at least one storage circuit and which circuitry comprises:

at least one storage area in said storage circuit, in which storage area protected data relating to circuitry security are located;

mode setting means arranged to set said processor in one of at least two different operating modes, the mode setting means being capable of altering the processor operating mode;

storage circuit access control means arranged to enable said processor to access said storage area in which said protected data are located when a first processor operating mode is set; and

storage circuit access control means arranged to prevent said processor from accessing said storage area in which protected data are located when a second processor operating mode is set, thereby enabling said at least one processor to execute non-verified software downloaded into the circuitry.

2. The circuitry for providing data security according to claim 1, further comprising:

a timer arranged to control the time period during which the processor is in said second operating mode.

3. The circuitry for providing data security according to claim 1 or 2, further comprising:

authentication means arranged to authenticate software provided to the circuitry.

4. The circuitry for providing data security according to any of the preceding claims, further comprising:

means arranged to indicate in which mode the processor is operating.

5. The circuitry for providing data security according to any of the preceding claims, wherein said mode setting means comprise an application program.

6. The circuitry for providing data security according to any of the preceding claims, which circuitry is comprised in a mobile telecommunication terminal.

7. A method for providing data security in circuitry containing at least one processor and at least one storage circuit, which method comprises the steps of:

storing protected data relating to circuitry security in said storage circuit;

setting said processor in one of at least two different alterable operating modes;

enabling said processor to access said storage area in which said protected data are located when a first processor operating mode is set; and

preventing said processor from accessing said storage area in which protected data are located when a second processor operating mode is set, thereby enabling said at least one processor to execute non-verified software downloaded into the circuitry.

8. The method for providing data security according to claim 7, further comprising the step of:

controlling the time period during which the processor is in said second operating mode by means of a timer.

9. The method for providing data security according to claim 7 or 8, further comprising the step of:

authenticating software provided to the circuitry.

10. The method for providing data security according to any of claims 7-9, further comprising the step of:

indicating in which mode the processor is operating.

11. The method for providing data security according to any of claims 7-10, wherein the setting of said processor in one of at least two different alterable operating modes is performed by means of an application program.

12. The method for providing data security according to any of claims 7-11, wherein the circuitry containing at least one processor and at least one storage circuit is comprised in a mobile telecommunication terminal.

ABSTRACT

The present invention relates to circuitry and a method for providing data security, which circuitry contains at least one processor and at least one storage circuit. The invention is based on the idea that circuitry is provided in which a processor is operable in at least two different modes, one first secure operating mode and one second unsecure operating mode. In the secure mode, the processor has access to security related data located in various memories located within the circuitry. The access to these security data and the processing of them need to be restricted, since an intruder with access to security data could manipulate the circuitry. When testing and/or debugging the circuitry, access to security information is not allowed. For this reason, the processor is placed in the unsecure operating mode, in which mode it is no longer given access to the protected data.

1/2

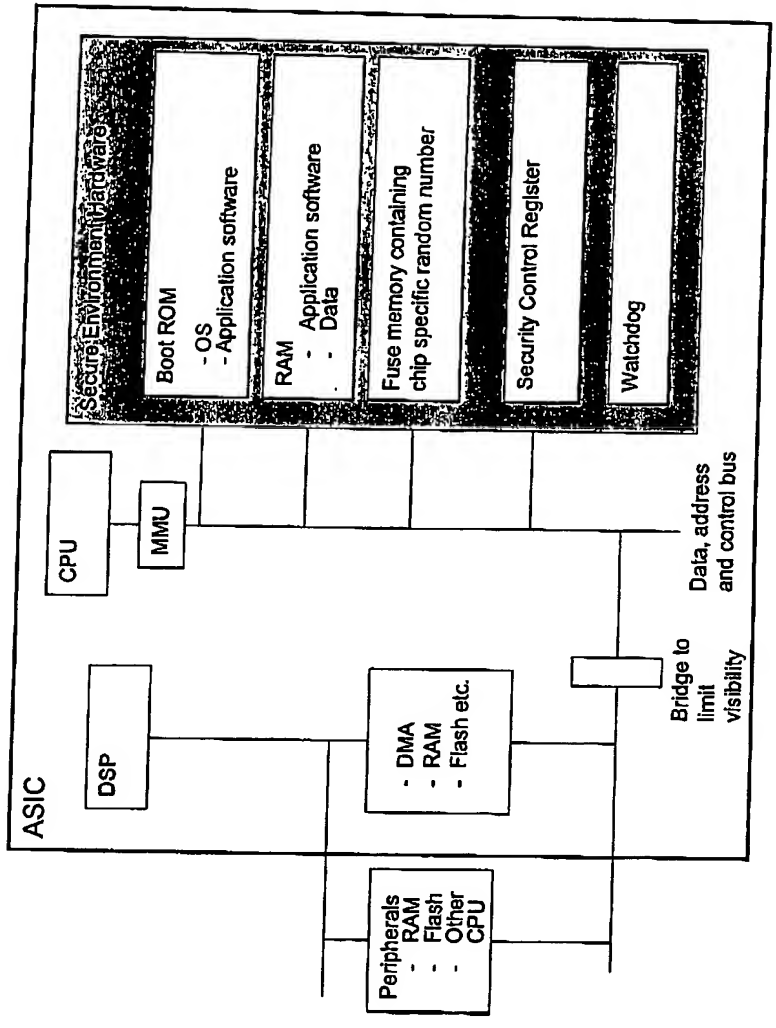
ASIC
Secure Environment Hardware
Boot ROM
- OS
- Application software
RAM
- Application software
- Data
Fuse memory containing chip specific random number
Security Control Register
Watchdog
CPU
MMU
DSP
- DMA
- RAM
- Flash etc.
Bridge to limit visibility
Data, address and control bus
Peripherals
- RAM
- Flash
- Other CPU

Fig. 1

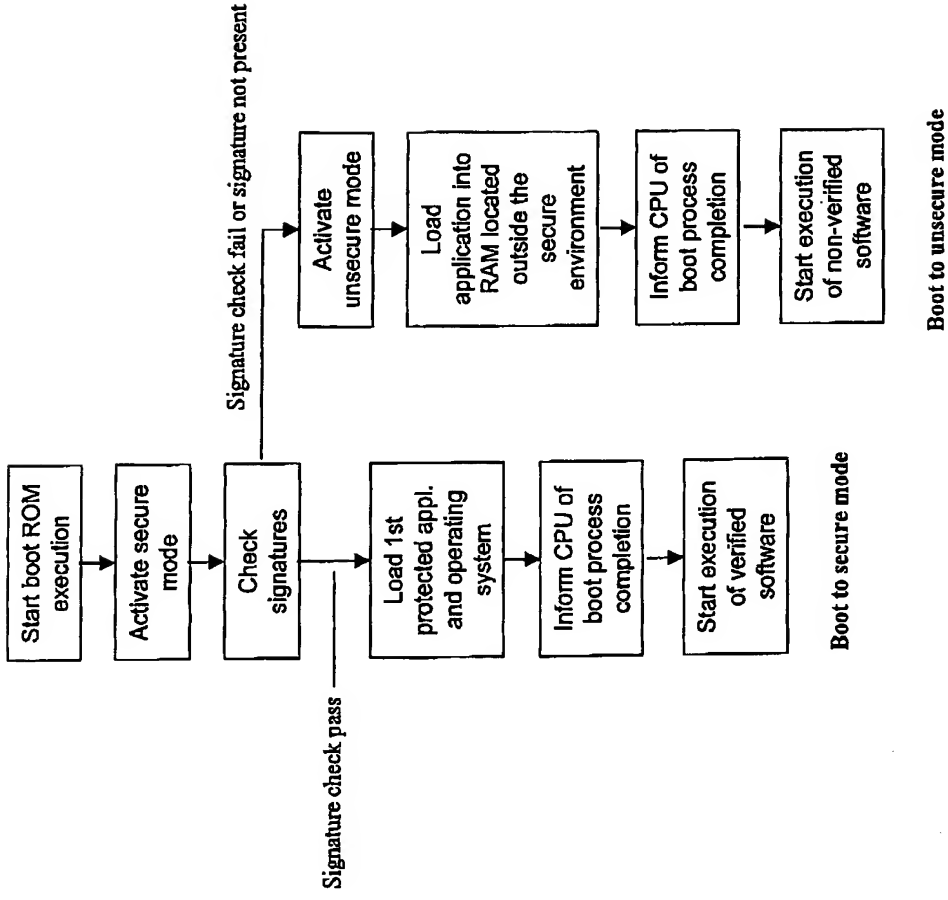
Start boot ROM execution
Activate secure mode
Check signatures
Signature check fail or signature not present
Activate unsecure mode
Load application into RAM located outside the secure environment
Inform CPU of boot process completion
Start execution of non-verified software
Boot to unsecure mode
Signature check pass
Load 1st protected appl. and operating system
Inform CPU of boot process completion
Start execution of verified software
Boot to secure mode

Fig. 2